

作業四：AES

學號：C24106082

姓名：陳宏彰

2022-10-04

1 結果

密鑰：Hj%N)6tgZ}9wrc*m

明文：National Cheng Kung University

隱藏的四個字元是%、6、}、*

2 完整程式碼

<https://github.com/simbafs/NCKU-IS-HW4>

3 過程

3.1 解密函數

首先要先寫出可以解出範例密文的解密函數，原本想透過 openssl 解密，但參數一直調不對。最後用 go 的標準函式庫 'crypto/aes' 解密。解密函數在 [aesUtil.go:54](#)

3.2 暴力搜尋

有了解密函數，接下來就只須要在暴力搜尋中用不同金鑰去嘗試，如果符合條件就印出來，程式碼在 [main.go:28](#)

3.3 限制條件

如果把所有解密出來的字串都印出來，數量會大到無法處理，因此需要加上限制條件。首先是公告的 **明文字首**，透過這個條件篩選，大概剩下 3000 個符合字串。接下來根據助教回信，明文都是有意義的字串，因此我們可以加上限制每個字元都必須是「可印的」，雖然不是精準的「有意義的」，但已經篩選到 52 個字串。最後根據兩個條件的篩選，可以看到有意義的字串只有「National Cheng Kung University」，因此這個應該就是原本的明文了。

解密出來的結果在 [plaintext:12](#)、密鑰在 [key:12](#)

```
100% | (268435456/268435456, 215759 it/s) [5/15]
~/git/ncku/12: H04  P main
~/git/ncku/12: H04  P main

1 0 Nad'uxE<88>pSq &&<96>/U rrcSASZAU0aE1
2 1 Na Yop>Ik LCB9 M*#B<8e>hQY[v]H<85>
3 2 Naauf<83><9a>NtB=xk0-y<94>h>ISi>Msc<A><89>
4 3 Najly<88>WYU<88>EAHU[?E77A<8e>h0<9e>]NB
5 4 NaeIs<9e>X<83>#4D1 E<9e> <A1> <0>[<82>E<9b>B&
6 5 Na<99>VW0 [/?]NHU0 AiyU ZQU<g0>Sv<90>
7 6 NaUilINS0<8a>CISSH<93>CIXU7a<81>0AUJsqw
8 7 NaU a.EgVM<8a>NE<9a>=<85>A<97>0n<8a>/ZMEI70<9f>
9 8 Na jAZ000a<92[?I]M<01>m<80>0<07>M<f<86>
9 9 NaID!<cx<91>=1b]w9S<80>0D0r43B7AD<S<83><8b>V
11 10 Na.'a:ITE0A0<96>[<91>0VAX0Xn[fpU<88>E&A&
12 11 National Cheng Kung University
13 12 Naa<9e>N<9e>0F<97>IVC0C0L<2>=<9f>B3 0iut
14 13 Na<99>E<80>NvJcc0m[?I]AHe<89>g<88>A<8e><99>I
15 14 NaU!%>*S<97>[?b<87>880SUV<8f>V1<8e><93><97> Nx%E
16 15 Na'fuz.X1<96><92>A<83> Id<9a><97>g<81>qv<99>VEU0
17 16 Napx<94>M0gAqBA<86><9e>f<9d><8c>pd<8d><92>h<80>f<93>
18 17 Na0WJ00S1[?bb>A&E00<85>NvU<91>811<94>
19 18 Naa<88>A<9e><89><9f>A<86>E<96>B<86>W<9e><8d>EvE<8
20 19 NaIE0000<9b>A<8b>g'X(0<81>0<88>6<84>f<82>B<8c>vnr*d
21 20 Na4DEA0Q0=404)Up!vS<S<e<[U<8d>hH1n
22 21 Naa<9b>NS0eVrd<9c>0r<9b><80>2]S'0sA<80><98>F'~
23 22 Naa<96>0U<99> B<92>WY000000<86>A<N<8e>8b>WY00~
24 23 Na<81>ro0XA<8c>h<94>=dr U<95>[a]E0<96>B<81>U<95>
25 24 Naa<8a>=92>W<85>U0gF<85>'0<8c>2[0<87>=0;Nb7
26 25 NaRa<9e>m<8b>Tn[?<97>00b1<85>Up0<N<C0<=36eU
27 26 Na<94>?NEXA100<93>A[0< E? UUD0<8e><84>0<99>f
NORMAL plaintext unix | latin1 no ft 22% 12:3
NORMAL key unix | utf-8 no ft 22% 12:1
> 5 0:nvim* 10/05 21:02 CPU:3.9% MEM:48% 0.03 0.08 0.14
```

NCKU Moodle 正體中文 (zh-tw)

陳宏彰

首頁 / 個人化首頁 / 簡歷National Cheng Kung University

將頁面重設為預設狀態 自訂首頁

用戶的詳細資料

編輯個人資料

電子郵件信箱
c24106082@gs.ncku.edu.tw

帳號
c24106082

課程簡節

課程簡介

1111_F731200_1111_資訊安全 INFORMATION SECURITY(1111_F731200)

1111_F711110_1111_程式設計 (一) PROGRAM DESIGN(1)(1111_F711110)

META_1111_RB55100_1111_體育室課程簡表(母課程) (META_1111_RB55100)

1111_A213200_2_1111_自由車 (男女) CYCLING(M + F)(1111_A213200_2)

1111_A910503_1111_倫理學 ETHICS(1111_A910503)

META_1111_C221110_A_1111_物理實驗 (一) PHYSICS EXPERIMENTS(1)(母課程) (META_1111_C221110_A)

1111_C221110_B_1111_物理實驗 (一) PHYSICS EXPERIMENTS(1)(1111_C221110_B)

1111_C221110_1111_生命學 (一) ASTONMULV

其它

討論區文章

討論區議題

報表

瀏覽器活動歷程

成績簡覽

登入活動

最後一次登入網站

2022年 10月 5日(Wed) 20:32 (1秒)